Application Owner / Customer Specific Security Responsibility Matrix (External Service, Cloud) v1.0										
Control Number and Name (FedRAMP Rev4 Workbook)		Control Baseline (LOW or MOD)	FedRAMP Defined Assignment/Selection Parameters	Additional FedRAMP Requirements and Guidance	Control Origination	Responsibility & Additional Notes				Comments
					Cloud Provider (C), DOI (D), GeoPlatform (G), Application Owner (A), share (combined letters) OR Not Applicable (N/A)	Cloud Provider	DOI	GeoPlatform Team/Contractors	Application Owner	
1.1. Access Control (AC)										
AC-1	Access Control Policy and Procedures	LOW	AC-1.b.1 [at least every 3 years]AC-1.b. 2 [at least annually]		CDGA	https://aws.amazon.com/compliance/fedramp/	Policy	Providing information requested for the controls	Consult your local security manager for your agency's specific policies and procedures	
AC-2	Account Management	LOW	AC-2j [at least annually]		CGA	https://aws.amazon.com/compliance/fedramp/		Document the different kinds of information system accounts that will be used in the system (e.g. admin, pr, coua, user, backup operator, guest) and then based on that assign/document 1. who are the system account managers (e.g. domain admins) 2. conditions for an employee to be part of special access groups or roles 3. approval process for new accounts 4. procedures for creating, enabling, modifying, disabling and removing accounts. 5. monitor/log account usage 6. review accounts for compliance at least annually. 7. process for reissuing shared/group accounts when membership changes." Need to show evidence that this is reviewed with in a defined frequency (quarterly? or yearly?)	Responsbile for accounts at the application level	
AC-2 (1)	Automated System Account Management	MOD			CGA					
AC-2 (2)	REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS	MOD	[No more than 30 days for temporary and emergency account types]		CGA					
AC-2 (3)	DISABLE INACTIVE ACCOUNTS	MOD	[90 days for user accounts]	Requirement: The service provider defines the time period for non-user accounts (e.g., accounts associated with devices). The time periods are approved and accepted by the Authorizing Official.	CGA					
AC-2 (4)	AUTOMATED AUDIT ACTIONS	MOD			CGA					
AC-3	Access Enforcement	LOW			CGA	https://aws.amazon.com/compliance/fedramp/		Document authorization process for accounts listed in AC-2	Responsible for having an authorization process for customer managed accounts that are used for authentication to customer managed resources like web applications	
AC-4	Information Flow Enforcement	MOD			CGA					
AC-5	Separation of Duties	MOD			CGA					
AC-6	Least Privilege	MOD			CGA					
AC-6 (1)	AUTHORIZE ACCESS TO SECURITY FUNCTIONS	MOD			CGA					

AC-6 (2)	NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS	MOD	[all security functions]	AC-6 (2). Guidance: Examples of security functions include but are not limited to: establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters, system programming, system and security administration, other privileged functions.	CGA					
AC-6 (5)	PRIVILEGED ACCOUNTS	MOD			CGA					
AC-6 (9)	AUDITING USE OF PRIVILEGED FUNCTIONS	MOD			CGA					
AC-6 (10)	PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS	MOD			CGA					
AC-7	Unsuccessful Login Attempts	LOW	AC-7a [not more than three] [fifteen minutes] AC-7b [locks the account/node for thirty minutes]		CGA	https://aws.amazon.com/compliance/fedramp/		3 failed login attempts in 15 minutes followed by 30 minute lockout. DOI STIGs should cover this on the local OS, AD handles for other user accounts, need to document how this is enforces in remaining situations not covered by STIG or AD	For any local accounts, DB accounts, web app accounts etc that are not based in AD and therfore not subjected to global STIG settings, The customer must set local accounts to those settings designated.	Evidence: may need to request screenshots showing the system enforces this.
AC-8	System Use Notification	LOW	Parameter: See Additional Requirements and Guidance.	Requirement: The service provider shall determine elements of the cloud environment that require the System Use Notification control. The elements of the cloud environment that require System Use Notification are approved and accepted by the Authorizing Official (AO). Requirement: The service provider shall determine how System Use Notification is going to be verified and provide appropriate periodicity of the check. The System Use Notification verification and periodicity are approved and accepted by the AO.Guidance: If performed as part of a Configuration Baseline check, then the % of items requiring setting that are checked and that pass (or fail) check can be provided. Requirement: If not performed as part of a Configuration Baseline check, then there must be documented agreement on how to provide results of verification and the necessary periodicity of the verification by the service provider. The documented agreement on how to provide verification of the results are approved and accepted by the AO.	CGA	https://aws.amazon.com/compliance/fedramp/		DOI Login banner, privacy policy and security policy links (screen shot showing it is in place) where possible	DOI Application owners: DOI Banner and policy links; Other agencies??	
AC-10	Concurrent Session Control	MOD	[three (3) sessions for privileged access and two (2) sessions for non-privileged access]		CGA	https://aws.amazon.com/compliance/fedramp/		Platform managed resources	Application or customer control resources	
AC-14	Permitted Actions Without Identification/ Authentication	LOW			CGA	https://aws.amazon.com/compliance/fedramp/		Any actions performed without identification or authentication needs to be documented with rationale. Or statement of assurance that no acctions can be performed on the system without identification or authentication	Any actions performed without identification or authentication needs to be documented.	
AC-17 (1)	AUTOMATED MONITORING / CONTROL	MOD			GA					

AC-17 (2)	PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION	MOD			GA					
AC-17 (3)	MANAGED ACCESS CONTROL POINTS	MOD			GA					
AC-17 (4)	PRIVILEGED COMMANDS / ACCESS	MOD			GA					
AC-19 (5)	FULL DEVICE / CONTAINER-BASED ENCRYPTION	MOD			A					
AC-21	Collaboration and Information Sharing	MOD			A					
AC-22	Publicly Accessible Content	LOW	AC-22d. [at least quarterly]		A				Application owners should follow the publishing guidelines of their bureau.	
1.3. Audit and Accountability (AU)										
AU-1	Audit and Accountability Policy and Procedures	LOW	AU-1.b.1 [at least every 3 years]AU-1.b. 2 [at least annually]		CDGA	https://aws.amazon.com/compliance/fedramp/	Policy	Providing information reuqested for the controls	Consult your local security manager for your agency's specific policies and procedures	
AU-2	Auditable Events	LOW	AU-2a. [Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes];AU-2d. [organization-defined subset of the auditable events defined in AU-2 a. to be audited continually for each identified event].		CGA	https://aws.amazon.com/compliance/fedramp/		Need to capture the information in column D. Should be covered by using cloudwatch/cloud trail	Applicable STIGs and DOI hardening standards and guidelines	Evidence: screen shot of audit logs showing this information is captured
AU-2 (3)	REVIEWS AND UPDATES	MOD	AU-2 (3). [Assignment: organization-defined frequency] Parameter: [annually or whenever there is a change in the threat environment]	Guidance: Annually or whenever changes in the threat environment are communicated to the service provider by the Authorizing Official.	CGA					
AU-3	Content of Audit Records	LOW	Audit records must contain what type of event occurred, when, where, the source, the outcome, and the identity of any individuals or subjects associated with the event.		CGA	https://aws.amazon.com/compliance/fedramp/		Need to capture the information in column D. Should be covered by using cloudwatch/cloud trail	Applicable STIGs and DOI hardening standards and guidelines	Evidence: screen shot of audit logs showing this information is captured
AU-3 (1)	ADDITIONAL AUDIT INFORMATION	MOD	AU-3 (1). [Assignment: organization-defined additional, more detailed information] Parameter: [session, connection, transaction, or activity duration; for client-server transactions, the number of bytes received and bytes sent; additional informational messages to diagnose or identify the event; characteristics that describe or identify the object or resource being acted upon]	AU-3 (1). Requirement: The service provider defines audit record types. The audit record types are approved and accepted by the Authorizing Official.Guidance: For client-server transactions, the number of bytes sent and received gives bidirectional transfer information that can be helpful during an investigation or inquiry.						
AU-4	Audit Storage Capacity	LOW			CGA	https://aws.amazon.com/compliance/fedramp/				Evidence: screenshot showing amount of disk space for audit logs
AU-5	Response to Audit Processing Failures	LOW	AU-5b. [Assignment: Organization-defined actions to be taken] Parameter: [low-impact: overwrite oldest audit records; moderate-impact: shut down]		CGA	https://aws.amazon.com/compliance/fedramp/		Designate a list of officials to receive automated notification (ISSO,OPS Admins) when there is a failure in audit processing. (environment is currently FISMA low, overwrite oldest logs, assuming that the failure is of a storage nature, will change when GP can host moderate)	Consult your bureau security manager for audit and accountability policy and procedures	

AU-6	Audit Review, Analysis, and Reporting	LOW	AU-6a. [Assignment: organization-defined frequency] Parameter: [at least weekly]		CGA	https://aws.amazon.com/compliance/fedramp/		Review audit records at least weekly, report findings to designated list (ISSO,OPS team, CSIRT?)	Customer will need to review any web or custom app logs outside the scope of GP management and report their findings internal to their team, document who it is being reported to etc. customers are also responsible for reporting any findings of interest to the GP team and GP/cloud ISSO.	
AU-6 (1)	PROCESS INTEGRATION	MOD			CGA					
AU-6 (3)	CORRELATE AUDIT REPOSITORIES	MOD			CGA					
AU-7	Audit Reduction and Report Generation	MOD			CGA					
AU-7 (1)	Automatic Processing	MOD			CGA					
AU-8	Time Stamps	LOW			CGA	https://aws.amazon.com/compliance/fedramp/		Document time source	Document time source	
AU-8 (1)	SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE	MOD	AU-8 (1). [http://tf.nist.gov/tf-cgi/servers.cgi] <At least hourly>	AU-8 (1). Requirement: The service provider selects primary and secondary time servers used by the NIST Internet time service. The secondary server is selected from a different geographic region than the primary server. Requirement: The service provider synchronizes the system clocks of network computers that run operating systems other than Windows to the Windows Server Domain Controller emulator or to the same time source for that server.Guidance: Synchronization of system clocks improves the accuracy of	CGA					
AU-9	Protection of Audit Information	LOW			CGA	https://aws.amazon.com/compliance/fedramp/		Develop documentation t	If the customer plugs their logging function into GP process, the customer should not have to document this control - inherited, but if they do not, they will need to document as well.	
AU-9 (4)	ACCESS BY SUBSET OF PRIVILEGED USERS	MOD			GA					
AU-11	Audit Record Retention	LOW	AU-11. [at least ninety days]	AU-11. Requirement: The service provider retains audit records on-line for at least ninety days and further preserves audit records off-line for a period that is in accordance with NARA requirements.	CGA	https://aws.amazon.com/compliance/fedramp/		90 days	90 days	
AU-12	Audit Generation	LOW	AU-12a. [all information system and network components where audit capability is deployed/available]		CGA	https://aws.amazon.com/compliance/fedramp/		Evidence: audit log output	Evidence: audit log output	
1.4. Assessment and Authorization (CA)										
CA-1	Security Assessment and Authorization Policies and Procedures	LOW	CA-1.b.1 [at least every 3 years]CA-1.b.2 [at least annually]		CDGA	https://aws.amazon.com/compliance/fedramp/	Policy	Participation in developing and implementing security controls	Consult your local security manager for your agency's specific policies and procedures	
CA-2	Security Assessments	LOW	CA-2b. [at least annually] CA-2d [individuals or roles to include FedRAMP PMO]		CDGA	https://aws.amazon.com/compliance/fedramp/	Direct activities	Participate in assessment	Participate in activities.	
CA-2 (1)	INDEPENDENT ASSESSORS	LOW	Added to NIST Baseline for "Low" FedRAMP baseline.	For JAB Authorization, must be an accredited 3PAO	CDGA	https://aws.amazon.com/compliance/fedramp/	OIG	Participate in assessment	Participate in activities.	
CA-3	Information System Connections	LOW	CA-3c. 3 Years / Annually and on input from FedRAMP		CDGA	https://aws.amazon.com/compliance/fedramp/	Review and approval	As needed for connections to other information systems	Customers will be required to obtain ISAs with any cooperators for access other than general public access to the application.	

CA-3 (5)	RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS	MOD		For JAB Authorization, CSPs shall include details of this control in their Architecture Briefing	Not Applicable					
CA-5	Plan of Action and Milestones	LOW	CA-5b. [at least monthly]	CA-5 Guidance: Requirement: POA&Ms must be provided at least monthly.	CDGA	https://aws.amazon.com/compliance/fedramp/	Review and approval	Participate in reviews and closure activities	Customers are required to provide their own Plan of Action and Milestones (POAMs) to include any managment, technical, and operational risks that could compromise the confidentiality, integrity and availability of the applications being hosted	
CA-7 (1)	INDEPENDENT ASSESSMENT	MOD			GA					
1.5. Configuration Management (CM)										
CM-1	Configuration Management Policy and Procedures	LOW	CM-1.b.1 [at least every 3 years]CM-1.b.2 [at least annually]		CDGA	https://aws.amazon.com/compliance/fedramp/	Policy	Providing information requested for the controls	Consult your local security manager for your agency's specific policies and procedures	
CM-2	Baseline Configuration	LOW			CGA	https://aws.amazon.com/compliance/fedramp/		Develop a baseline configuration for all components in the information system.	Develop a baseline configuration for all components that are customer managed.	
CM-2 (1)	REVIEWS AND UPDATES	MOD	CM-2 (1) (a). [at least annually]CM-2 (1) (b). [to include when directed by Authorizing Official]		GA					
CM-2 (3)	RETENTION OF PREVIOUS CONFIGURATIONS	MOD			GA					
CM-2 (7)	CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS	MOD			A					
CM-3	Configuration Change Control	MOD		Requirement: The service provider establishes a central means of communicating major changes to or developments in the information system or environment of operations that may affect its services to the federal government and associated service consumers (e.g., electronic bulletin board, web status page). The means of communication are approved and accepted by the Authorizing Official.CM-3e Guidance: In accordance with record retention policies and procedures.	GA					
CM-3(2)	Configuration Change Control | Test / Validate / Document Changes	MOD	The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.		GA					
CM-4	Security Impact Analysis	LOW			CGA	https://aws.amazon.com/compliance/fedramp/		Analysis of the security impacts of making the change	Security Impact Analysis is required to be performed in order to measure and analyze the associated risks prior to an approved system change to be deployed in production.	Who is responsible for this and how is it approved in a multi-tenant environment?
CM-5	Access Restrictions for Change	MOD			CGA					
CM-6	Configuration Settings	LOW	CM-6a. [See CM-6(a) Additional FedRAMP Requirements and Guidance]	CM-6a. Requirement: The service provider shall use the Center for Internet Security guidelines (Level 1) to establish configuration settings or establishes its own configuration settings if USGCB is not available.CM-6a. Requirement: The service provider shall ensure that checklists for configuration settings are Security Content Automation Protocol (SCAP) validated or SCAP compatible (if validated checklists are not available).CM-6a. Guidance: Information on the USGCB checklists can be found at: http://usgcb.nist.gov/usgcb_faq.html#usgcbfaq_usgcbfdcc .	CGA	https://aws.amazon.com/compliance/fedramp/				

CM-8	Information System Component Inventory	LOW	CM-8b. [at least monthly]	CM-8 Requirement: must be provided at least monthly or when there is a change.	CGA	https://aws.amazon.com/compliance/fedramp/		Way to inventory system components and appropriate tag items that are tied to customers	Can use AWS tagging or cloud checkr reports	
CM-8 (1)	UPDATES DURING INSTALLATIONS / REMOVALS	MOD			CGA					
CM-8 (3)	AUTOMATED UNAUTHORIZED COMPONENT DETECTION	MOD	CM-8 (3) (a). [Continuously, using automated mechanisms with a maximum five-minute delay in detection.]		CGA					
CM-8 (5)	NO DUPLICATE ACCOUNTING OF COMPONENTS	MOD			CGA					
CM-9	Configuration Management Plan	MOD			GA					
CM-10	Software Usage Restrictions	LOW			CGA	https://aws.amazon.com/compliance/fedramp/		Software licenses that are just "baked" in like OS on instances will automatically be tracked and charged in AWS . Any other software that is not instant license from AWS can be tracked. monitoring for P2P usage will occur at the Sophos (and later TIC) for outbound traffic.	Customers are responsible for ensuring that only licensed software is utilized on all workstations and desktops and users are prohibited by policy of installing unlicensed software. Customers are responsible for monitor continuously for such violations.	Use software according to contract and license agreement, do not copy or distribute, and monitor for P2P file sharing to limit the distribution of copyrighted material.
CM-11	User-Installed Software	LOW	CM-11.c. [Continuously (via CM-7 (5))]		CGA	https://aws.amazon.com/compliance/fedramp/			Customers are responsible for ensuring that only licensed software is utilized on all workstations and desktops and users are prohibited by policy of installing unlicensed software. Customers are responsible for monitor continuously for such violations.	
1.6. Contingency Planning (CP)										
CP-1	Contingency Planning Policy and Procedures	LOW	CP-1.b.1 [at least every 3 years]CP-1.b.2 [at least annually]		CDGA	https://aws.amazon.com/compliance/fedramp/	Policy	Providing information reuqested for the controls	Consult your local security manager for your agency's specific policies and procedures	
CP-2	Contingency Plan	LOW	CP-2d. [at least annually]	Requirement: For JAB authorizations the contingency lists include designated FedRAMP personnel.	CGA	https://aws.amazon.com/compliance/fedramp/		Coordinate between DOI staff and contractors	Consult your local security manager for your agency's specific policies and procedures	
CP-3	Contingency Training	LOW	CP-3.a. [10 days]CP-3.c. [at least annually]		CGA	https://aws.amazon.com/compliance/fedramp/		Provide contingency plan training to all those employees who will be integral to activating and carrying out the plan.	Customers are responsbile for their own applications and coordination with GP staff	
CP-4	Contingency Plan Testing and Exercises	LOW	CP-4a. [at least annually for moderate impact systems; at least every three years for low impact systems] [functional exercises for moderate impact systems; classroom exercises/table top written tests for low impact systems]	CP-4a. Requirement: The service provider develops test plans in accordance with NIST Special Publication 800-34 (as amended); plans are approved by the Authorizing Official prior to initiating testing.	CGA	https://aws.amazon.com/compliance/fedramp/		Contingency plan test annually	Customers should test annually or meet their Bureau requirements	

CP-9	Information System Backup	LOW	CP-9a. [daily incremental; weekly full] CP-9b. [daily incremental; weekly full] CP-9c. [daily incremental; weekly full]	CP-9. Requirement: The service provider shall determine what elements of the cloud environment require the Information System Backup control.Requirement: The service provider shall determine how Information System Backup is going to be verified and appropriate periodicity of the check.CP-9a. Requirement: The service provider maintains at least three backup copies of user-level information (at least one of which is available online) or provides an equivalent alternative.CP-9b. Requirement: The service provider maintains at least three backup copies of system-level information (at least one of which is available online) or provides an equivalent alternative.CP-9c. Requirement: The service provider maintains at least three backup copies of information system documentation including security information (at least one of which is available online) or provides an equivalent alternative.	CGA	https://aws.amazon.com/compliance/fedramp/		Covered under managed services	Covered under managed services but customers are responsbile for anything not covered under the managed services	
CP-10	Information System Recovery and Reconstitution	LOW			CGA	https://aws.amazon.com/compliance/fedramp/		Covered under managed services	Covered under managed services but customers are responsbile for anything not covered under the managed services	
CP-10 (2)	TRANSACTION RECOVERY	MOD			CA					
1.7. Identification and Authentication (IA)										
IA-1	Identification and Authentication Policy and Procedures	LOW	IA-1.b.1 [at least every 3 years]IA-1.b.2 [at least annually]		CDGA	https://aws.amazon.com/compliance/fedramp/	Policy	Providing information requested for the controls	Consult your local security manager for your agency's specific policies and procedures	
IA-2 (8)	NETWORK ACCESS TO PRIVILEGED ACCOUNTS - REPLAY RESISTANT	MOD			A					
IA-2 (11)	REMOTE ACCESS - SEPARATE DEVICE	MOD	The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [Assignment: organization-defined strength of mechanism requirements].		DGA					
IA-3	Device Identification and Authentication	MOD			DGA					
IA-5 (1)	PASSWORD-BASED AUTHENTICATION	LOW	IA-5 (1) (a). [case sensitive, minimum of twelve characters, and at least one each of upper-case letters, lower-case letters, numbers, and special characters]IA-5 (1) (b). [at least one]IA-5 (1) (d). [one day minimum, sixty day maximum]IA-5 (1) (e). [twenty four]		CGA	https://aws.amazon.com/compliance/fedramp/		Responsible to enforce for anything using password-based authentication	Responsbile for accounts at the application level	
IA-6	Authenticator Feedback	LOW			CGA	https://aws.amazon.com/compliance/fedramp/		Document any occurrances where this cannot be enforced	Responsible for customer managed resources and applications	
IA-7	Cryptographic Module Authentication	LOW			CGA	https://aws.amazon.com/compliance/fedramp/		Modules needs to be FIPS 140-2 compliant.	If the customer uses cryptographic modules in their applications outside of what is provided by GP and AWS (e.g. Linux/Apach SSL/TLS), those moldules must be officially FIPS-140-2 validated: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm	

IA-8	Identification and Authentication (Non-Organizational Users)	LOW			CA	See FedRAMP package			GP will not support any non-organizational users. This control falls to Amazon and the customer. Customers should use an e-authentication mechanism in their application if it authenticates any non-organizational users. For smaller sets of users, managing a custom or internal authentication mechanism may suffice.	must uniquely identify and authenticate non-organizational users. The simplest approach to do ing this is to use an e-authentication mechanism to authenticate non-organization users. Is it correct to say that GP will not support non-organizational users?
IA-8 (2)	ACCEPTANCE OF THIRD-PARTY CREDENTIALS	LOW			A	https://aws.amazon.com/compliance/fedramp/			Authenticated public web sites being served from GP must use only 3rd party authentication credentials issued by non-federal entities which are FICAM approved. http://www.idmanagement.gov/approved-identity-services . If the customer uses an e-authentication mechanism for their application to authenticate non-organizational users (IA-8 line 164), that mechanism must be FICAM approved. (see the above URL	
IA-8 (3)	USE OF FICAM-APPROVED PRODUCTS	LOW			A	https://aws.amazon.com/compliance/fedramp/			Authenticated public web sites being served from GP must use only 3rd party authentication system components which are also FICAM approved. IA-8(2) was about identity providers, this control is about system components which authenticate users with 3rd party FICAM approved credentials. http://www.idmanagement.gov/. Customer must use only FICAM approved components for authentication of non-organizational users to applications: References: OMB Memoranda 04-04, 11-11, 10-06-2011; FICAM Roadmap and Implementation Guidance; FIPS Publication 201; NIST Special Publications 800-63, 800-116; National Strategy for Trusted Identities in Cyberspace; Web: http://idmanagement.gov	
IA-8 (4)	USE OF FICAM-ISSUED PROFILES	LOW			A	https://aws.amazon.com/compliance/fedramp/			Customer must configure the FICAM approved components according to FICAM approved implementation templates. http://www.idmanagement.gov/	
1.8. Incident Response (IR)										
IR-1	Incident Response Policy and Procedures	LOW	IR-1.b.1 [at least every 3 years]IR-1.b.2 [at least annually]		CDGA	https://aws.amazon.com/compliance/fedramp/	Policy	Providing information requested for the controls	Consult your local security manager for your agency's specific policies and procedures	
IR-6	Incident Reporting	LOW	IR-6a. [US-CERT incident reporting timelines as specified in NIST Special Publication 800-61 (as amended)]	Requirement: Reports security incident information according to FedRAMP Incident Communications Procedure.	CDGA	https://aws.amazon.com/compliance/fedramp/		All suspected security incidents must be reported to the DOI CSIRT within 1 hour	ROB	
1.9. Maintenance (MA)										
MA-3 (2)	INSPECT MEDIA	MOD			CDA					
1.12. Planning (PL)										

PL-4	Rules of Behavior	LOW	PL-4c. [At least every 3 years]		CGA	https://aws.amazon.com/compliance/fedramp/		Covered in contract, or by DOI policy for employees and contractor staff	Needs to sign ROB	
PL-4 (1)	SOCIAL MEDIA AND NETWORKING RESTRICTIONS	MOD			DGA					
1.14. Risk Assessment (RA)										
RA-2	Security Categorization	LOW			CGA	LOW/MOD offering	Oversight	LOW offering now, MOD evetually	Application owner's responsibility to determine and appropriately deploy (Information types workbook)	
RA-5	Vulnerability Scanning	LOW	RA-5a. [monthly operating system/infrastructure; monthly web applications and databases] RA-5d. [high-risk vulnerabilities mitigated within thirty days from date of discovery; moderate-risk vulnerabilities mitigated within ninety days from date of discovery]	RA-5a. Requirement: an accredited independent assessor scans operating systems/infrastructure, web applications, and databases once annually.RA-5e. Requirement: to include the Risk Executive; for JAB authorizations to include FedRAMP	CDGA	https://aws.amazon.com/compliance/fedramp/	Oversight?	Infrastructure level scanning monthly, monthly application and database, mitigation services	Application-level mitigation	How is scanning information desceminated and to who? Does there need to be a user type added to the user table? Who is responsible for mitigation?
RA-5 (1)	UPDATE TOOL CAPABILITY	MOD			CDGA					
RA-5 (5)	PRIVILEGED ACCESS	MOD	RA-5 (5). [operating systems / web applications / databases] [all scans]		DGA					
1.15. System and Services Acquisition (SA)										
SA-2	Allocation of Resources	LOW			CDGA	https://aws.amazon.com/compliance/fedramp/	DOI FCH	Covered in contract	Customer works with GP team/ vendor	
SA-4 (1)	FUNCTIONAL PROPERTIES OF SECURITY CONTROLS	MOD			DGA					
SA-4 (2)	DESIGN / IMPLEMENTATION INFORMATION FOR SECURITY CONTROLS	MOD	[to include security-relevant external system interfaces and high-level design]		DGA					
SA-4 (9)	FUNCTIONS / PORTS / PROTOCOLS / SERVICES IN USE	MOD			GA					
SA-5	Information System Documentation	LOW			CGA	https://aws.amazon.com/compliance/fedramp/		Collect administrative and user documentation from the vendor, document attempts to get it if they have none, protect it in accordance with risk management strategy and give it to organizational roles with defined roles.	Customer obtains software or other services from vendors, such as on the AWS marketplace, they should obtain administrative and user documentation for the product	
SA-8	Security Engineering Principles	MOD			GA					
SA-9 (2)	IDENTIFICATION OF FUNCTIONS / PORTS / PROTOCOLS / SERVICES	MOD	SA-9 (2). [All external systems where Federal information is processed, transmitted or stored]		A					
SA-10	Developer Configuration Management	MOD	SA-10a. [development, implementation, AND operation]	SA-10e. Requirement: for JAB authorizations, track security flaws and flaw resolution within the system, component, or service and report findings to organization-defined personnel, to include FedRAMP.	GA					
SA-11	Developer Security Testing	MOD			GA					
1.16. System and Communications Protection (SC)										
SC-1	System and Communications Protection Policy and Procedures	LOW	SC-1.b.1 [at least every 3 years]SC-1.b. 2 [at least annually]		CDGA	https://aws.amazon.com/compliance/fedramp/	Policy	Providing information requested for the controls	Consult your local security manager for your agency's specific policies and procedures	
SC-4	Information in Shared Resources	MOD			CGA					
SC-5	Denial of Service Protection	LOW			CGA	https://aws.amazon.com/compliance/fedramp/		Implement and documen	Customers have responsibility to prevent DoS through SQL injection, etc. by secure coding practices.	
SC-10	Network Disconnect	MOD	SC-10. [no longer than 30 minutes for RAS-based sessions or no longer than 60 minutes for non-interactive user sessions]		CGA					

SC-13	Use of Cryptography	LOW	FIPS-validated or NSA-approved cryptography]		CGA	https://aws.amazon.com/compliance/fedramp/		All cryptography controls in use must be FIPS or NSA validated.	If the customer uses any cryptographic modules in their application (e.g. SSL) it must be FIPS or NSA validated.	
SC-18	Mobile Code	MOD			A					
SC-21	Secure Name/ Address Resolution Service (Recursive or Caching Resolver)	LOW			CGA	https://aws.amazon.com/compliance/fedramp/		Implement	Implement for customer controlled resources	This control requires clients and endpoints to use secure DNS services only when resolving addresses. DNS client resolvers either perform validation of DNSSEC signatures, or clients use authenticated channels to recursive resolvers that perform such validations. This will likely need to be documented as part of DOI STIGS for Windows and Linux OS. Customers must ensure that instances use DNSSEC once it is available. Weakness in AWS. POAM?
SC-23	Session Authenticity	MOD			CGA					
1.17. System and Information Integrity (SI)										
SI-1	System and Information Integrity Policy and Procedures	LOW	SI-1.b.1 [at least every 3 years]SI-1.b.2 [at least annually]		CDGA	https://aws.amazon.com/compliance/fedramp/	Policy	Providing information requested for the controls	Consult your local security manager for your agency's specific policies and procedures	
SI-2	Flaw Remediation	LOW	SI-2c. [Within 30 days of release of updates]		CGA	https://aws.amazon.com/compliance/fedramp/		Vulerability scanning, IEM, SEP, ect., managing patching process	Consult your local security manager for your agency's specific policies and procedures	
SI-2 (2)	AUTOMATED FLAW REMEDIATION STATUS	MOD	SI-2 (2). [at least monthly]		CGA					
SI-3	Malicious Code Protection	LOW	SI-3.c.1 [at least weekly] [to include endpoints]SI-3.c.2 [to include alerting administrator or defined security personnel]		CGA	https://aws.amazon.com/compliance/fedramp/		Install malicous code protection on all endpoints, UTM malware detection for network	Consult your local security manager for your agency's specific policies and procedures	
SI-3 (1)	CENTRAL MANAGEMENT	MOD			CGA					
SI-3 (2)	AUTOMATIC UPDATES	MOD			CGA					
SI-4 (2)	AUTOMATED TOOLS FOR REAL-TIME ANALYSIS	MOD			CGA					
SI-4 (5)	SYSTEM-GENERATED ALERTS	MOD		SI-4(5) Guidance: In accordance with the incident response plan.	CGA					
SI-10	Information Input Validation	MOD			A					
SI-11	Error Handling	MOD			GA					
SI-12	Information Output Handling and Retention	LOW			CGA	https://aws.amazon.com/compliance/fedramp/		Implement Records management for all relevant information contained in or generated by the information system as defined in the annual FISSA+ training.	Consult your local security manager for your agency's specific policies and procedures	
SI-16	Memory Protection	MOD			CGA					